Cybersecurity and Maintaining Public Trust

December 2018

Kevin Smith

Chief Information Officer

United States Census Bureau

U.S. Department of Commerce
Economics and Statistics Administration
U.S. CENSUS BUREAU
census.gov

2020 Census Cybersecurity
Goals

Maintain positive **public perception/ trust** of our data security

Defend, detect, and respond to cyberthreats

Design systems to adjust quickly as threats emerge

Approach implementation strategically and refine as needed.

End to End Cybersecurity

Our end to end approach to security will **continually be refined** as threats emerge & evolve

We will:

- **Maintain** the public's trust and confidence by protecting their data and keeping them informed
- **Defend** against cyberthreats through technology and partnerships
- Adjust solutions accordingly within our **flexible design**
- Work with federal and industry partners to help us **refine our approach** and fill gaps

2020 Census Cybersecurity

Our Cybersecurity Focus

Partners

Secure Connection (Protect and Detect)

- *Working with Industry and Federal Government to ensure scalable and secure federal network connection*

Improve Cybersecurity Posture (Identify, Protect, Detect)

- *Improve technology, knowledge and processes*

Strengthen Incident Response (Protect, Detect, Respond, Recover)

- *Advance ability to continually Identify, Protect, Detect, Respond and Recover from possible cyber threats*

2020 Census Cybersecurity

End to End Security - NIST Cybersecurity Framework

NIST Cybersecurity Framework v1.1

- Released in April 2018
- Aligned with
  - Federal - NIST SP 800-53 Rev. 4
  - Business Governance - COBIT 5
  - Security Standards
    - CIS CSC - Center for Internet Security
    - ISA – International Society of Automation
    - ISO/IEC - International Standards Organization/ International Electrotechnical Commission

Recovery Planning (RC.RP)
Communications (RC.CO)
Improvements (RC.IM)

Business Environment (ID.BE)
Governance (ID.GV)
Risk Management Strategy (ID.RM)
Supply Chain Risk Management (ID.SC)
Asset Management (ID.AM)
Risk Assessment (ID.RA)

Response Planning (RS.RP)
Communications (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)

Awareness and Training (PR.AT)
Information Protection Processes and Procedures (PR.IP)
Identity Management, Authentication and Access Control (PR.AC)
Data Security (PR.DS)
Maintenance (PR.MA)
Protective Technology (PR.PT)

Detection Processes (DE.DP)
Anomalies and Events (DE.AE)
Security Continuous Monitoring (DE.CM)

2020 Census Cybersecurity

End to End Security – Where Partners Play

Federal

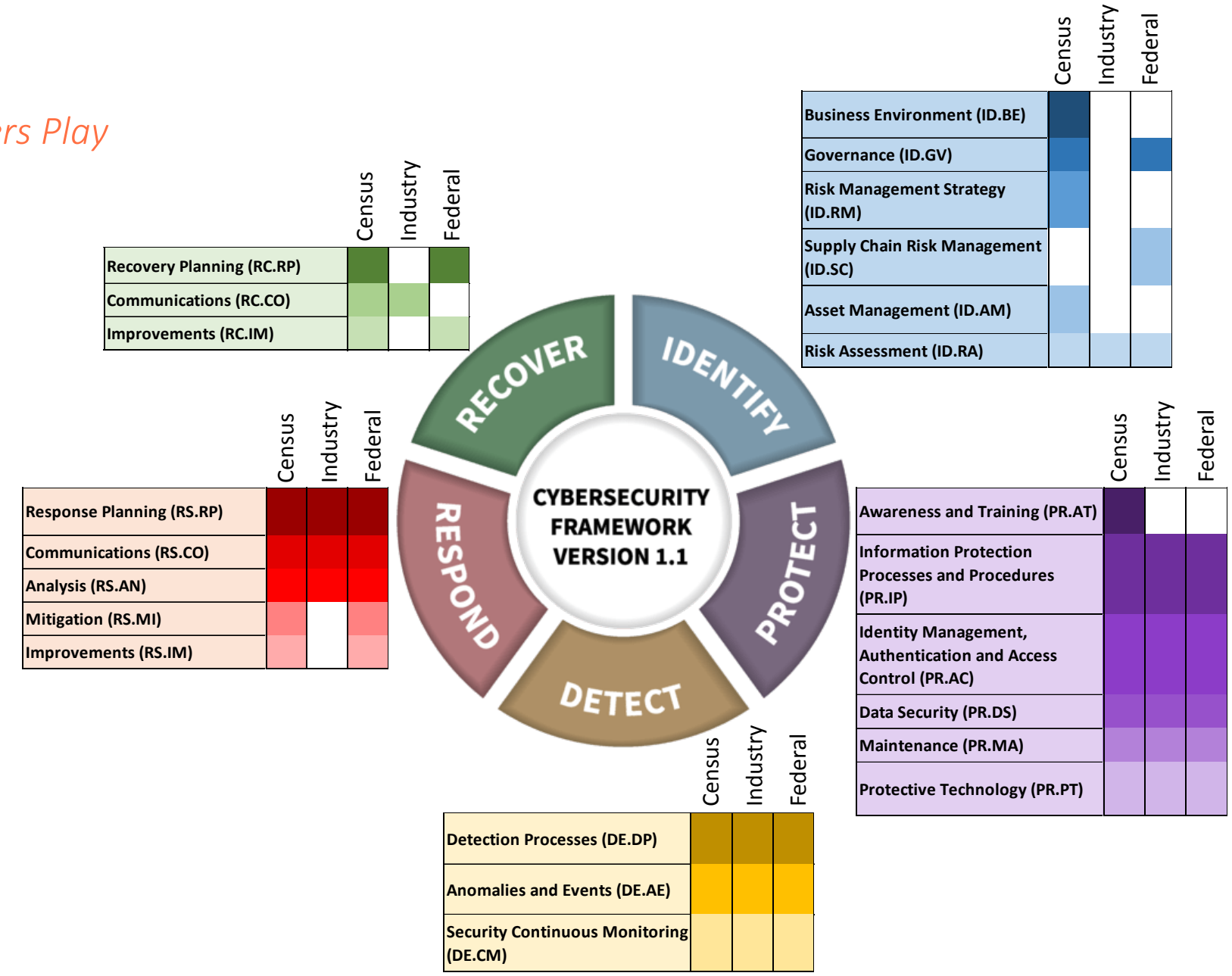
- Contributes in Identify, Protect, Detect, Respond, and Recover

Industry

- Focused in Protect, Detect
- Conduct Tests in Respond
- Assist Communications in Recover

Census

- Leads and contributes to Protect, Detect, Respond, and Recover

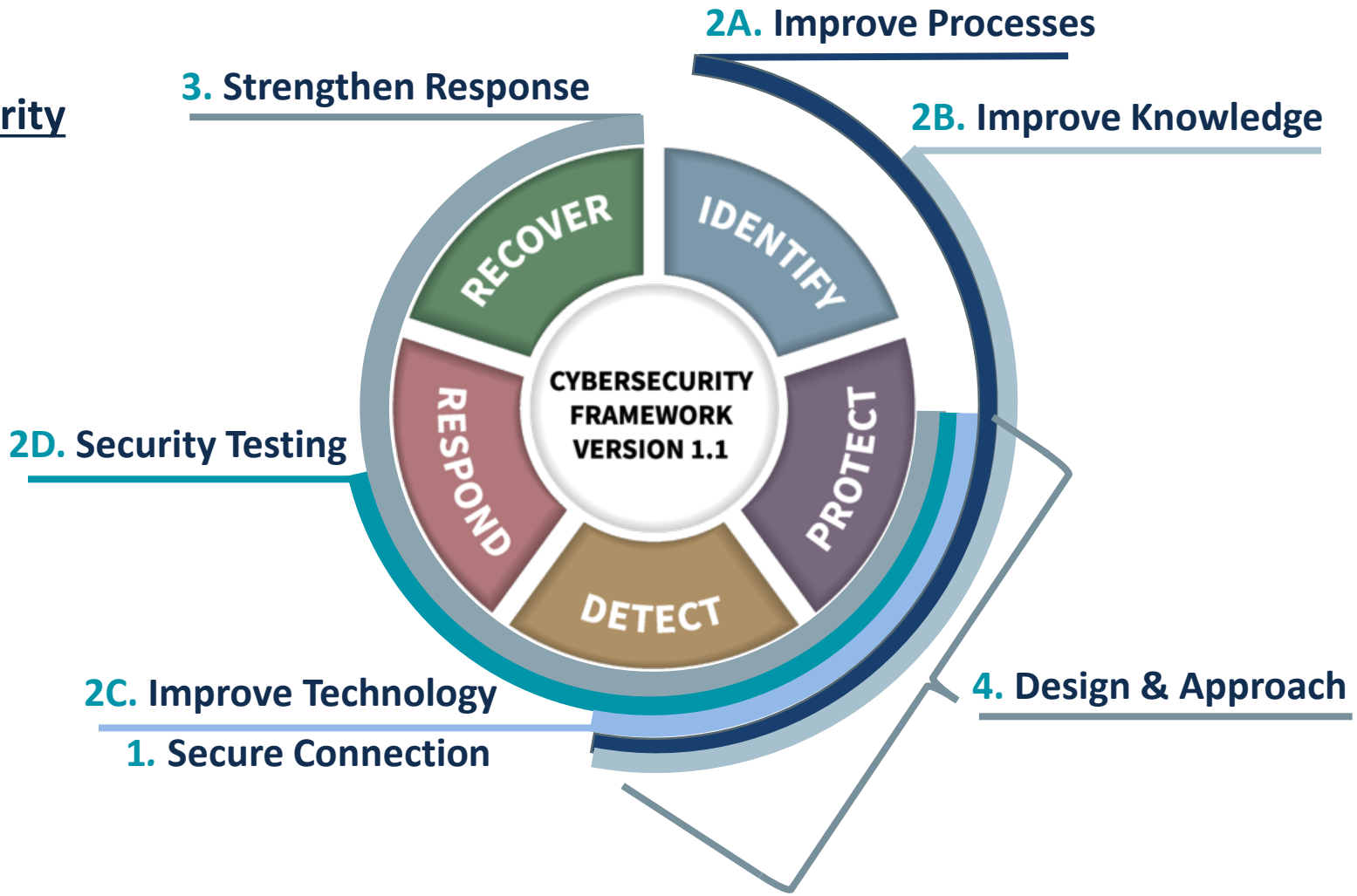


2020 Census Cybersecurity

End to End Security – Focus Areas

Focus Areas Cover End to End Cybersecurity

1. **Secure Connection**
2. **Improving Cybersecurity Posture**
   - A. Improving Processes and Procedures
   - B. Improving Knowledge
   - C. Improving Technology
   - D. Validating with Security Testing
3. **Strengthen Incident Response**
4. **Design and Approach**
   - Balance Constraints



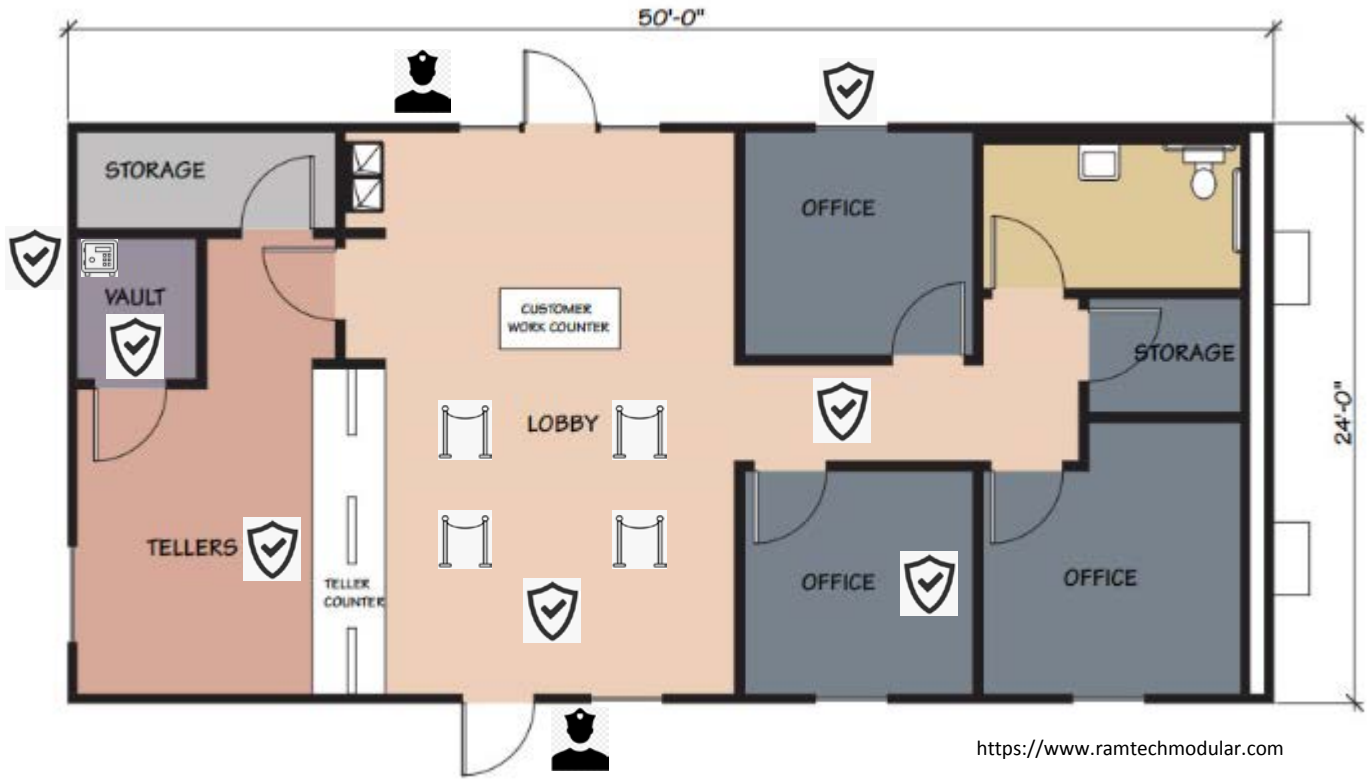
2020 Census Cybersecurity

Design - Balancing User Experience and Security

Back to the Basics

Employ physical security techniques in logical world

- **Flow** Intentionally manage data flow to see unexpected behavior (hallways)
- **Contain** Layered entry with appropriate level of security for the area (doors, walls)
- **Sustain** Isolate areas to handle interactions (lines, tellers, guards)
- **Secure** Lock down valuables behind closed doors (vaults, safes)



https://www.ramtechmodular.com

2020 Census Cybersecurity

Approach – Operationalize Security to Control More of What We Can

Look for What I Know Could Happen --- Define Actions of What I Can Do

Approach

- Design – Intentional behavior flows
- Decide - Determine bad behavior
- Share – Behavior with partners
- Watch – Everyone look for behavior
- Respond – Immediate, Less

Behavior

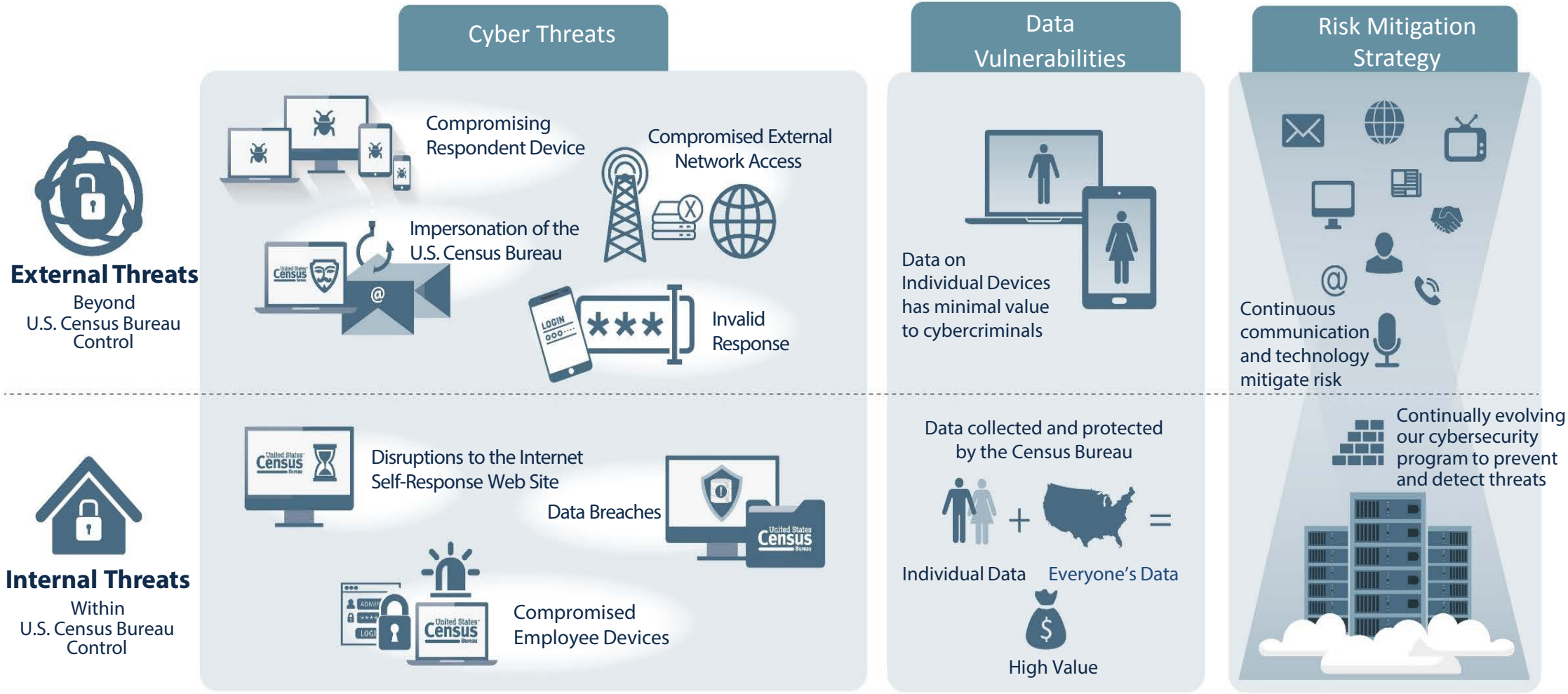
- Who is not supposed to here?
- What is not using it normally?
- When is access is not expected?
- Where do we not expect access?
- How much is not expected?
- What is not sustaining expectations?

If we see it, we do not wait. We contain it before it starts and sustain things running.

Additional Details

2020 Census Cybersecurity

Our Cybersecurity Threat Areas



External Cyber Threat Mitigation

Relying on Partnerships

External Threat Mitigation Strategies	
Compromising Respondent Device	▪ Minimal storing of data on device ▪ Encryption of data in-transit for website communications ▪ Proactive public outreach and awareness campaign
Compromised External Network Access	▪ Proactive monitoring of site performance and activity ▪ Proactive monitoring for unauthorized or unusual connection attempts ▪ Industry and interagency coordination and information sharing
Impersonation of U.S. Census	▪ Proactive identification of rogue websites ▪ Interagency coordination and information sharing ▪ Proactive public outreach and awareness campaign
Invalid Response	▪ Automated analysis of individual responses to identify irregularities ▪ Analysis of identified irregularities ▪ Data flow analysis

Internal Cyber Threat Mitigation

Monitoring and Directly Responding

Internal Threat Mitigation Strategies	
Disruption to the Internet Self-Response Web Site	▪ Monitoring for traffic spikes and unusual activity in systems/applications ▪ Proactive identification of malicious traffic and robots ▪ Cyber threat intelligence (federal, commercial, state, and local government) ▪ Designed to sustain self response services ▪ Use of Distributed Denial of Service (DDoS) protection services
Data Breaches	▪ Monitoring for irregular data flows ▪ Monitoring for unauthorized access ▪ Encryption of data in-transit and at-rest ▪ System/application penetration testing ▪ Security management, monitoring, and analytics ▪ Timely patch management ▪ Cyber awareness training ▪ Proactive public outreach and awareness campaign
Compromised Employee Devices	▪ Encryption of data in-transit and at-rest ▪ Remote wipe capability ▪ Monitoring user activity and detection of malicious end user ▪ Two factor authentication ▪ Phishing tests

2020 Census Cybersecurity

End to End Security - NIST Cybersecurity Framework v1.1

IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

2020 Census Cybersecurity

End to End Security - NIST Cybersecurity Framework v1.1

PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

2020 Census Cybersecurity

End to End Security - NIST Cybersecurity Framework v1.1

RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

2020 Census Cybersecurity

End to End Security – Some Examples of Partner Involvement

- Risk and Vulnerability Assessment
- High Value Asset (HVA) Assessment Program
- CyberStat Program
- .gov Cybersecurity Architecture Review (.govCAR)
- Federal Information Security Management Act (FISMA) CIO Metrics (Annual)
- Cybersecurity Cross-Agency Priority (CAP) Goals Report (Quarterly)
- Cyber Services Liaisons (CSLs) and Support Requests
- Insider Threat Assessment
- Authority to Operate (ATO) Process

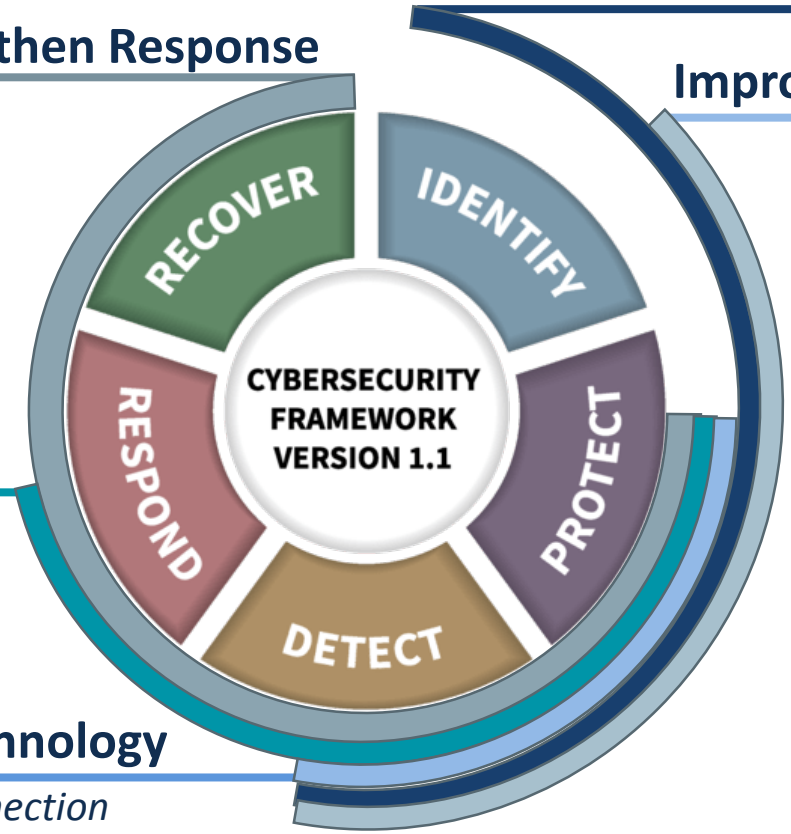
Improve Processes

Strengthen Response

- National Cybersecurity and Communications Integration Center (NCCIC) Cybersecurity Exercises (IR Tabletop)
- National Cyber Incident Response Plan (NCIRP) Support
- Federal Cyber Incident Notification Reporting
- Federal Incident Response Evaluation (FIRE)
- Operationalize Security
- Security Operations
- Secure Response Communications
- Enterprise Incident Response Plan
- 2020 Continuity of Operations Plan
- 2020 Disaster Recovery Plan
- Security Operations Center Capabilities
- Census Cyber Tabletop Exercises
- Cybersecurity Communications
- 2020 Recovery Planning Playbooks

Improve Knowledge

- Cybersecurity Threat Intelligence Integration Center (ODNI)
- Cybersecurity Unified Coordination Group (CUCG)
- Continuous Diagnostic and Mitigation (CDM) Program
- Automated Indicator Sharing
- Homeland Security Information Network (HSIN)
- Trusted Internet Connection (TIC) Initiative
- National Cybersecurity Protection System (NCPS) (Einstein)
- Threat Intelligence
- Supply Chain Risk Assessment (DOC)
- Threat Intelligence
- Social Media Monitoring
- Security Training



Security Testing

- Penetration Testing and Phishing Exercises
- Red Team Assessment
- Penetration Tests
- Bug Bounty (Internet Self Response)

Improve Technology

Secure Connection

- Security Architecture Review
- Internet Self Response Assessment
- Internet Self Response Design
- Threat Mitigation Technology
- System Architecture
- Monitoring Services
- Continuous Monitoring
- Cloud Trusted Internet Connection / Einstein (Pilot)

Federal Government

Industry

- ***Census***

United States Census Bureau

U.S. Department of Commerce
Economics and Statistics Administration
U.S. CENSUS BUREAU
census.gov